61200740L1-29.4A
March 2009

ADTRAN

Configuration Guide

Security Dashboard

This troubleshooting guide provides information regarding the ADTRAN Operating System (AOS) Security Dashboard. This feature simplifies the collection and display of network information that is relevant to the security of the network. This guide is an overview of the information presented in the Security Dashboard using the Web-based graphical user interface (GUI) and commands available from the AOS command line interface (CLI).

This guide consists of the following sections:

Introduction to the Security Dashboard

The AOS Security Dashboard feature has been designed as a visual representation of the network security threats blocked by the AOS firewall. Common examples of information displayed in the dashboard are how many threats have been encountered, the first appearance of a threat, and frequency of a threat over time. Previously, a record of these threats was either not available or only available by searching through SysLog messages.

The Security Dashboard provides a general overview of network security status that allows the user to quickly and easily assess security threats and firewall status. The Security Dashboard is a collection of information, and is not intended to provide recommendations regarding additional security or risk management measures.

This guide contains a detailed list of available CLI commands related to the Security Dashboard, as well as screenshots from the GUI that provide an outline of the information available within the feature.

Hardware and Software Requirements and Limitations

The initial implementation of the Security Dashboard feature occurred in AOS version 17.5. It should be noted that the majority of the information available through the Security Dashboard feature has been available in earlier AOS versions through less direct methods than the Security Dashboard interface.

The Security Dashboard feature is enabled by default on all AOS products that support the firewall.

Limitations

The Security Dashboard feature does not make recommendations concerning the management of network security threats.

Accessing the Security Dashboard Using the GUI

The following section describes the various components of the Security Dashboard feature as interfaced through the GUI. Screenshots and descriptions of each component are used to outline the navigation and layout of the feature.

Sidebar

After logging on to the unit via the Web interface using the appropriate user name and password, the Security Dashboard feature can be accessed using the sidebar. The sidebar is visible on the left hand side of the GUI as shown in Figure 1 on page 3, and contains options that allow administration of the device. Each sidebar selection can be expanded to display submenus by selecting the plus sign next to the item.

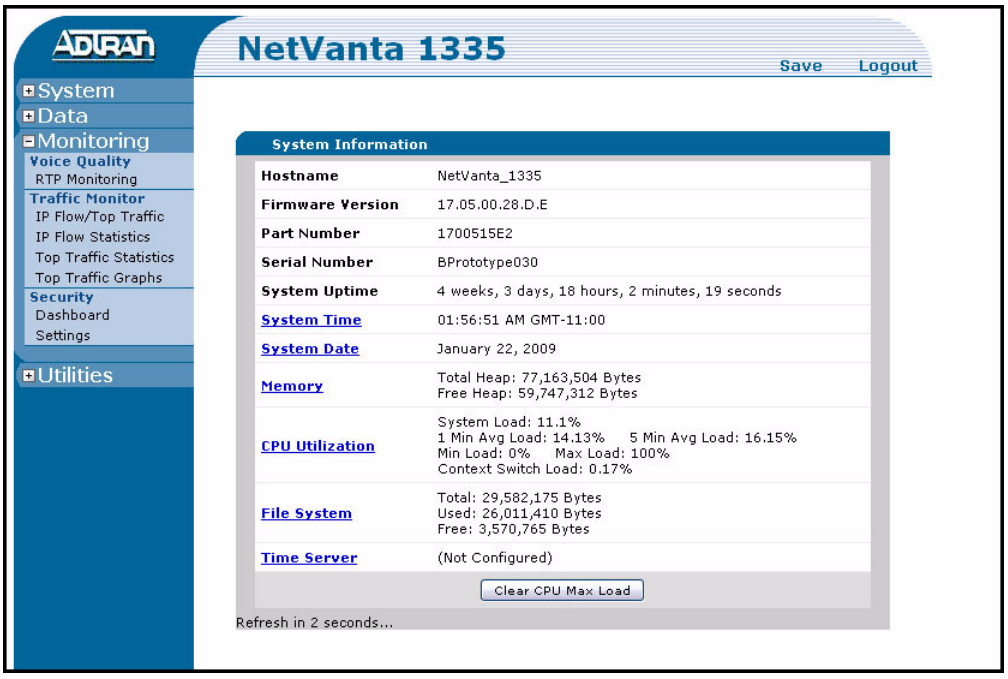

Figure 1. System Information Menu with Expanded Sidebar

Dashboard

To access the Security Dashboard, navigate to **Monitoring > Security > Dashboard**. There are two sections to the Security Dashboard menu: the **Threat Statistics** section and the **Security Zone Statistics** section. These sections are visible in Figure 2 on page 4.

Threat Statistics

The **Threat Statistics** section displays all potential security threats using a tabbed viewing pane. The tabs organize the threats into three sections: **Observed**, **All**, and **Ignored**. The **Observed** tab shows only threats that have been observed by the network device. This is the default tab when the Security Dashboard is opened. The **All** tab shows all potential threats that can be observed within the Security Dashboard, those that have been observed, those that have not been observed, and those in the global filter. The **Ignored** tab shows those threats that are being ignored by the global filter. For more information on the global filter, refer to *Security Dashboard Settings* on page 5.

Threats can be added to the global filter by selecting the **Ignore** button to the right of the threat listing in the viewing pane. Once a threat has been ignored, it will show up in the **All** and **Ignored** tabs, but not in the **Observed** tab.

Next to each listed security threat are four columns of information. These columns are **Hits**, **First Observed**, **Last Observed**, and **Weight**. The **Hits** column indicates the number of times the given threat has occurred since the threat was last cleared. **First Observed** and **Last Observed** indicate the time the given threat was first observed and most recently observed, respectively. **Weight** indicates, on a scale of 1 to 10, the potential severity of the threat. The higher the number, the more serious the threat may be. Threat weight is also indicated by color. Threats listed in red (10 to 8) are considered high, yellow (7 to 4)

medium, and green (3 to 1) low. Threats can be sorted by each of these four columns, as well as by the threat ID (located to the left of the threat description) by selecting the column title.

At the bottom of the **Threat Statistics** section is the **Clear all observed threats** button. Selecting this button restarts the counter for all threat hits, as well as the clearing **First Observed** and **Last Observed** times.

> NOTE
>
> *Selecting a threat name in the **Description** column of the **Threat Statistics** section opens a new browser window that contains all information from the **Threat Statistics** columns, as well as a detailed description of that particular threat.*

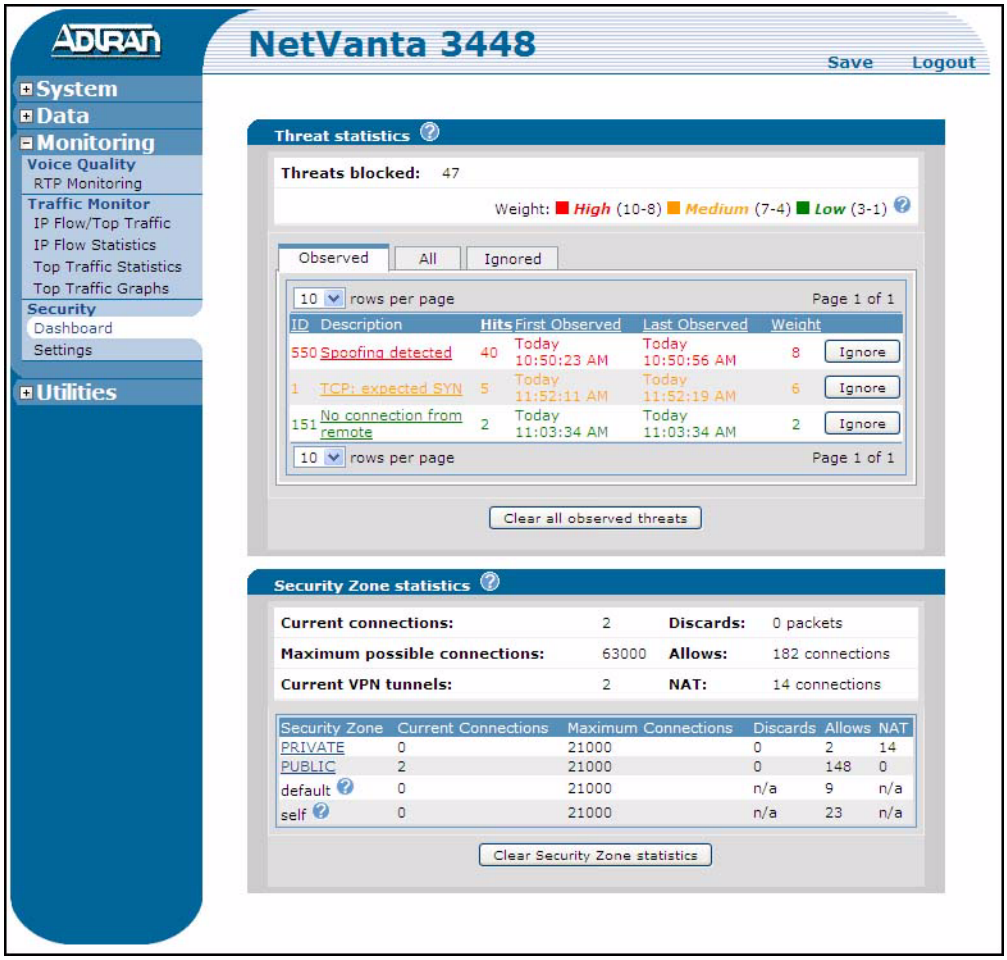

Figure 2. Security Dashboard

Security Zone Statistics

The **Security Zone Statistics** section is located below the **Threat Statistics** section as seen in Figure 2. In the GUI, Security Zones are equivalent to policy classes in the CLI. This section displays statistics related to established security zones. It displays statistical totals for all zones in the top portion while breaking down the statistics by individual zones in the bottom portion. All statistics can be cleared by selecting the **Clear Security Zone Statistics** button. For additional information concerning policy classes and security zones, refer to the applicable configuration guides or the *AOS Command Reference Guide* located on the *AOS Documentation* CD shipped with your ADTRAN product or online at www.adtran.com.

Security Dashboard Settings

To access the **Security Dashboard Settings** section, navigate to **Monitoring > Security > Settings** as seen in Figure 3 on page 6. This section contains a complete list of all threats that can be monitored with the Security Dashboard feature. They are listed in descending order of threat weight and then by ascending threat ID in the case of threats with the same weight. Global filter settings are indicated by a check mark located in the box in the far left column. All threats with a check mark are currently being filtered and statistics are not being collected for those threats. Any global filter settings that have been changed can be saved by selecting the **Apply** button located at the top and bottom of the window. To reset the form to its original settings when the page was loaded, select the **Reset** button located next to the **Apply** button.

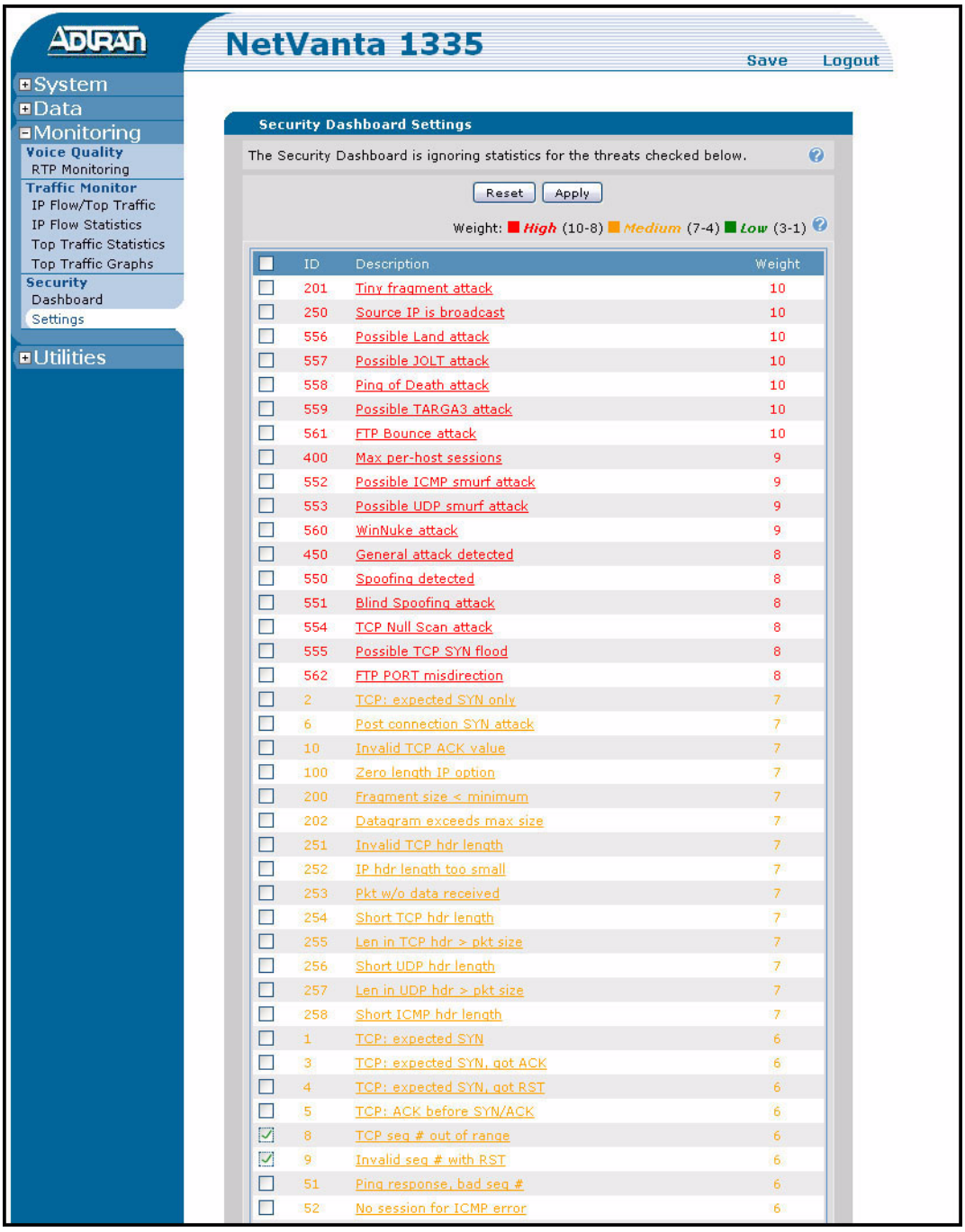

Figure 3. Security Dashboard Settings

Accessing the Security Dashboard in the CLI

The following section outlines the procedure for viewing Security Dashboard data using the CLI. Due to the nongraphical nature of the CLI, the Security Dashboard is referred to as the Security Monitor. The data presented through the CLI is identical to the data presented through the GUI. No configuration is necessary to view Security Dashboard (Security Monitor) data from the CLI, but a variety of options can be configured for viewing and clearing threat data.

The CLI can be accessed by several different methods. A VT100 terminal, a terminal emulation program on a PC, or Telnet can all be used. In order to access any AOS unit you must know the login information. The IP address of the unit is also required if accessing the unit using Telnet. For more information on connecting to your AOS unit, refer to the *AOS Command Reference Guide* located on the *AOS Documentation* CD shipped with your ADTRAN product or online at www.adtran.com.

Security Dashboard CLI commands are entered from several different modes. The Enable mode or the Global Configuration mode are used for the majority of the commands. The **color** and **stats-filter** commands are entered from the IP Security Monitor Configuration mode. A password is required to enter the Enable mode.

Show Commands

Security Dashboard (Security Monitor) information is displayed in the CLI using **show** commands. All **show** commands are entered from the Enable mode. To display security threat data in the CLI, use one of the **show ip security** commands, enumerated below. The **show ip security** command has a variety of arguments that can be used to display different sets of data. This threat data can be displayed for any available VPN routing and forwarding (VRF), a named VRF, or the default VRF. Refer to *Security Dashboard Show Commands* on page 9 for a complete list of options.

Additional **show** commands are available to display data relevant to network security. A complete listing of these commands can be found in the table *Additional Security Show Commands* on page 9.

Show Command Example

The following example displays security threat data for the default VRF for the tiny fragment attack threat, whose threat ID is 201:

```
>enable
Password:
#show ip security threats 201
Collected since: 25 Feb 2009 03:29:00 Current Time: 28 Feb 2009 22:17:22
Total threats blocked: 4

* denotes threats that are filtered globally
Weights: High: 10-8, Medium: 7-4, Low: 3-1
------------------------------------------------------------
Tiny fragment attack [00201], weight: 10
First observed: 25 Feb 2009 06:13:23 Hits: 52
Last observed: 28 Feb 2009 20:19:17 Avg: 13 / day
```

Configuration Commands

Configuration commands allow the user to alter the presentation of security threat data as it appears in the CLI. These alterations include adding or removing display color as an indicator of threat levels, and selective filtering of specific threats. Configuration commands are entered from the IP Security Monitor Configuration mode.

A complete listing of configuration commands can be found in the table *Configuration Commands* on page 10.

Configuration Command Example

The following example creates a new security monitor filter named **F1** and adds all threats to that filter.

```
>enable
Password:
#configure terminal
(config)#ip security monitor stats-filter F1

Creating new filter “F1”.

(config-secmon-filter)#threat all
(config-secmon-filter)#
```

Troubleshooting

To assist in troubleshooting, the **debug ip security monitor** command is available in the CLI to debug statistic collection associated with the timeline. The debug command is entered from the Enable mode. Entering this command causes debug messages to be displayed (real time) on the terminal (or Telnet) screen.

Turning on a large amount of debug information can adversely affect the performance of your unit.

The following is sample output from the **debug ip security monitor** command:

```
>enable
#debug ip security monitor
SECURITY_MONITOR.EVENTS Regular update: timeline interval scheduled to end at 23:00:16
SECURITY_MONITOR.EVENTS [ curr=269095, sched=272343 ]
SECURITY_MONITOR.EVENTS Regular update: timeline interval scheduled to end at 23:00:16
SECURITY_MONITOR.EVENTS [ curr=269154, sched=272343 ]
#
```

Clear commands are used to clear data collected by the IP security monitor. A complete listing of clear commands can be found in the table *Clear Commands* on page 11.

Command Summary Tables

Security Dashboard Show Commands

Prompt	Command	Description
#	**show ip security [vrf** <*name*> **| any-vrf] blocked-traffic timeline**	Displays a list of the number of threats blocked per hour and the number of packets discarded by policy classes per hour over the last 24 hours on the default VRF unless a named VRF or **any-vrf** is specified.
#	**show ip security [vrf** <*name*> **| any-vrf] threats [**<*id*> **| sort-by [first-observed | last-observed | weight | hits | id]] [realtime]**	Displays a list of all threats with descriptions, corresponding IDs, weights for threats that have been observed, the number of hits, the time it was first observed, and the time it was most recently observed. The list is sorted by hits unless the user chooses another option. All sorting options are in descending order except for IDs. A single ID can be entered to show a specific threat's information. The default VRF is implied unless a named VRF or **any-vrf** is specified.

Additional Security Show Commands

#	**show ip policy-sessions [vrf** <*name*> **| any-vrf] timeline**	Displays a list of the number of policy sessions created per hour and the peak number of concurrent policy sessions per hour over the last 24 hours on the default VRF unless a named VRF or **any-vrf** is specified.
#	**show crypto ipsec timeline**	Displays a list of the number of IPSec tunnels created per hour and the peak number of concurrent tunnels per hour over the last 24 hours. Virtual Private Network (VPN) features are available only in the enhanced feature set.
#	**show running-config ip security monitor**	Displays the portions of the running configuration that apply to security monitoring.

Configuration Commands

Prompt	Command	Description
(config)#	**ip security monitor**	Enters Security Monitor configuration mode.
(config-secmon)#	**[no] stats-filter** <*name*>	Applies the named security monitor filter globally. **No** removes the specified global filter. By default, no threats are filtered.
(config-secmon)#	**[no] color**	Displays threats on the terminal with a colored background corresponding to their threat level. This applies to the CLI only. Your VT100 terminal emulator must support VT100 color for this feature to work properly. The web GUI will always display color, regardless of this setting. **No** removes special coloring of threats. By default, no color is displayed.
(config)#	**[no] ip security monitor stats-filter** <*name*>	Creates a new security monitor filter and enters filter configuration mode. **No** deletes the specified security monitor filter. By default, no filters are defined.
(config-secmon-filter)#	**[no] threat [all | none | add** <*id(s)*> **| remove** <*id(s)*> **| except** <*id(s)*>**|** <*id(s)*>**]**	Filters a specific threat or multiple threats in a list or range. When a threat is added to a filter that is applied, its statistics are also cleared. Threat IDs are displayed in the output of the **show ip security threats** command. **All** adds all threats to the filter. **None** removes all threats from the filter. **Add** adds the specified threats to the filter (keeping any existing threats). **Remove** removes the specified threats from the filter (keeping any existing threats). **Except** adds all threats to the filter except the threats specified. <*id(s)*> filters only the specified threats, removing any existing threats. Valid range is **1** to **999**. **No** removes all threats from the filter (identical to threat **none**). By default, no threats are filtered.

Clear Commands

Prompt	Command	Description
#	**clear ip security monitor**	Clears all statistics associated with security monitor including policy statistics and excluding timeline and VPN statistics. The time of the clear is saved.
#	**clear ip security [vrf** <*name*> **| any-vrf] threats**	Clears the IP security threats list and restarts tracking of all threats. The time of the clear is saved.
#	**clear crypto ipsec sa peak**	Clears the peak IPSec SA count reached.
#	**clear crypto ike sa peak**	Clears the peak IKE SA count reached.

Debug Commands

Prompt	Command	Description
#	**debug ip security monitor**	Debugs statistic collection associated with the timeline.

